NUI Galway
OÉ Gaillimh

Semester 2 Examinations 2014/ 2015

Exam Code(s)	4BCT1, 1SWB1
Exam(s)	Year 4 BSc in Computer Science and Information Technology, Science without Borders
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Prof. G. Lyons Dr. M. Madden *Dr. C. Mulvihill

Instructions: Answer any 4 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	X	No	
MCQ	Yes		No	X
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes		No	X

PTO

1

(a) What is meant by the term 'block cipher'? (4 marks)

(b) Develop a simple model of the operation of a stream cipher, explaining the term 'keystream generator' in the course of your answer. (6 marks)

(c) Discuss any two ciphertext manipulations that could occur if deploying a block cipher in ECB (Electronic Code Book) mode. (10 marks)

2

(a) Briefly explain what is meant by a MAC (message authentication code).(5 marks)

(b) 'Digital signatures are about delivering a service aimed at data integrity and are not about encryption'. Explain what is meant by this claim. (7 marks)

(c) 'MAC algorithms could be based on a block cipher or a hash function'. Give a brief overview of either CBC-MAC or HMAC in the light of this statement. (8 marks)

3

(a) Briefly compare clock-based and sequence-based freshness mechanisms.(6 marks)

(b) 'Dynamic password schemes can address freshness and identity requirements through the use of PINs, tokens and challenge-response mechanisms.' Outline how authentication between a server and a user might work with such a scheme. (6 marks)

(c) Briefly outline what is meant by 'zero-knowledge entity authentication', using any analogy of your choice to illustrate your answer. (8 marks)

4

(a) 'Public-key systems often depend on a trapdoor one-way function.' Explain what is meant by this statement. (4 marks)

(b) In the context of public-key cryptography, explain what is meant by the terms 'X.509 public key certificate' and 'Certification Authority'. (6 marks)

(c) Alice is working on an assignment for her tutor Emma. Alice signs her assignment with her private signature key. She decides to consult Bob, who is in her class. Alice encrypts her signed assignment with Bob's public encryption key and sends the signed and encrypted assignment to Bob for a second opinion. Bob decrypts with his private decryption key, verifies Alice's signature with her public verification key, notices a flaw in the assignment, but sends the assignment on to Emma encrypted with Emma's public encryption key. As Alice signed the assignment she gets a low mark. Is there any way that this scenario can be counteracted? (10 marks)

PTO

5

(a) Explain what is meant by the terms ‘confidentiality’ and ‘integrity’ in the context of computer security. (6 marks)

(b) Briefly outline the ‘Chinese Wall’ model of access control, explaining what is meant by the term ‘conflict of interest classes’ in the course of your answer. (8 marks)

(c) What type of access control environment might be expected to enforce the so-called 'no read up' and 'no write down' (aka the ss-property and the *-property) access control properties between subjects and objects? Explain what is meant by 'no read up' and 'no write down' in the course of your answer. (6 marks)

6

(a) Briefly describe the following aspects of dealing with a suspect device: (1) sanitizing forensic disks (2) data carving and (3) examining log files. (9 marks)

(b) Explain the relevance of the ‘Daubert Criteria’ for computer forensics. (5 marks)

(c) ‘The presence of steganographic material on a device may lead to the defence of plausible deniability being invoked.’ Explain what is meant by this statement in the context of a forensic investigation. (6 marks)

7

In the context of the discussion found in the recent paper ‘Surreptitiously weakening cryptographic systems’ by Schneier, Fredrikson, Kohno and Ristenpart, or through your own investigations, briefly give your understanding of the following four cases: Lotus Notes, Dual Elliptic Curve DRBG, Debian OpenSSL PRNG, certificate checking double goto. (5 marks for each of the four - 20 marks in total)